

APERÇU DE L'ENTREPRISE

Les organisations échangent chaque jour des données sensibles à travers des milliers de canaux, de systèmes et de partenaires — pourtant, la plupart s'appuient encore sur des solutions ponctuelles fragmentées. Celles-ci créent des angles morts en matière de conformité, élargissent la surface d'attaque et privent les équipes de sécurité de la visibilité dont elles ont besoin. À mesure que l'IA accélère les workflows d'entreprise, l'écart de gouvernance se creuse : les données circulent plus vite que les politiques ne peuvent suivre, et les régulateurs n'attendent plus les violations pour sanctionner les défaillances de contrôle.

PRINCIPAUX DÉFIS

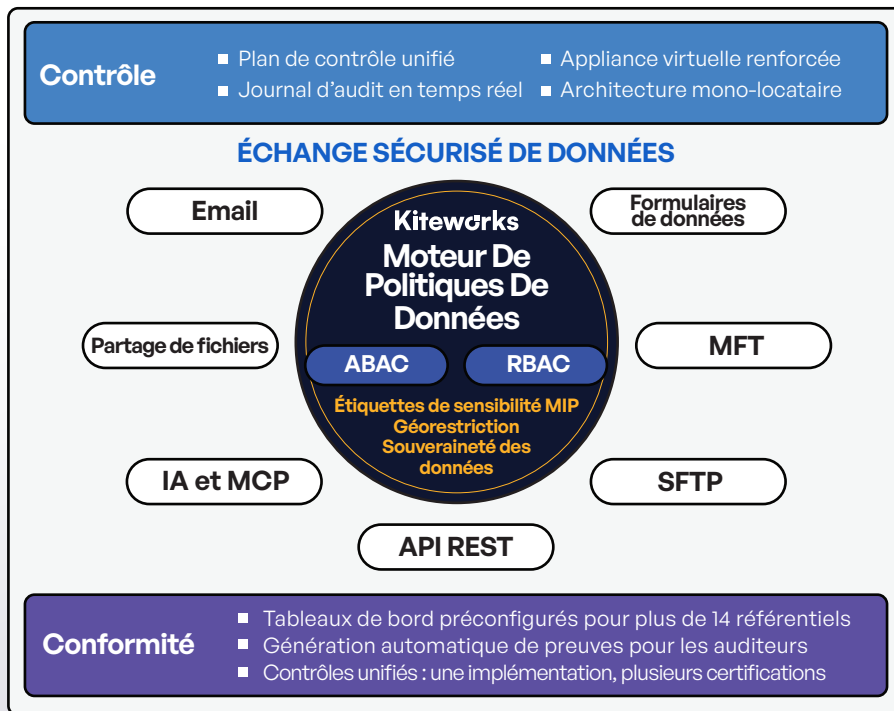
- 5 à 10** Outils déconnectés pour l'échange de contenus sensibles
- 4,45 M\$** Coût moyen d'une violation de données
- 1 sur 3** Incidents liés à la souveraineté des données au cours de l'année passée
- 33 %** Incidents liés à la souveraineté des données au cours de l'année passée
- 63 %** Incapacité à appliquer des limites d'accès aux données pour l'IA et les agents

CE QUE NOUS FAISONS

Kiteworks permet aux organisations de gérer efficacement les risques à chaque envoi, partage, réception et utilisation de données sensibles non structurées. La plateforme remplace les solutions ponctuelles fragmentées par un plan de contrôle unifié pour des échanges de données sécurisés — un moteur de politiques, un journal d'audit, une architecture de sécurité. Construite sur une appliance virtuelle renforcée avec une sécurité en profondeur, Kiteworks offre une gouvernance, une visibilité et une protection unifiées sur tous les canaux tout en étendant des contrôles de niveau entreprise aux workflows pilotés par l'IA.

Gouvernance Des Données IA

- Accès aux données pour l'IA et les agents selon un modèle zero trust
- RAG conforme pour les données d'entreprise
- Application des politiques ABAC/RBAC pour l'IA
- Journal d'audit en temps réel des accès IA
- Compatible avec toute plateforme IA compatible MCP



Connecteurs De Référentiels

Microsoft Office	CIFS/SMB File Shares
SharePoint	OneDrive
SFTP	Box
DropBox	Google Drive
Google Workspace	Google Cloud Storage
Amazon S3	Azure Blob
Wasabi	iManage
Salesforce	et plus encore

CMMC 2.0 | RGPD | HIPAA | NIS 2 | DORA | PIPEDA | ITAR | EU AI ACT | PCI DSS | ET PLUS ENCORE

Protection: Sécurité Centrée Sur Les Données (OpenTDF)

- Politiques intégrées aux fichiers—la protection accompagne les données
- Contrôles d'accès persistants quel que soit l'emplacement ou le système
- Alignement zero trust : chaque accès est vérifié à chaque fois

SafeEDIT: Édition Sans Possession

- Les parties externes modifient les documents sans les télécharger
- DRM nouvelle génération—les données ne quittent jamais votre environnement
- Plusieurs options de déploiement, y compris hébergement FedRAMP

CERTIFICATIONS ET VALIDATIONS

- FedRAMP High (en cours)
- FedRAMP Moderate
- SOC 2 Type II
- IRAP
- Cyber Essentials Plus
- ISO 27001/27017/27018
- FIPS 140-3
- BSI C5